

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 999 673 A2

(12)

EUROPEAN PATENT APPLICATION(43) Date of publication:
10.05.2000 Bulletin 2000/19(51) Int Cl.7: **H04L 12/58**, **H04L 29/06**,
H04L 12/26(21) Application number: **99308689.1**(22) Date of filing: **02.11.1999**(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI(30) Priority: **03.11.1998 US 185056**(71) Applicant: **NORTEL NETWORKS CORPORATION**
Montreal, Quebec H2Y 3Y4 (CA)(72) Inventors:
• **Mamros, Shawn**
Arlington, Massachusetts 02476 (US)
• **Hannigan Kerry M**
Boston, Massachusetts 02215 (US)(74) Representative: **Maury, Richard Philip et al**
Sommerville & Rushton,
Business Link Building,
45 Grosvenor Road
St. Albans, Herts AL1 3AW (GB)(54) **Protected keep alive message through the internet**

(57) A method and apparatus for determining the reachability of a remote computer from a local computer through a secured communications link through the Internet. In one embodiment, the secured ISAKMP/Oakley communications link is established between a remote computer and a local computer through the Internet. A protected keepalive message is transmitted by the local computer to the remote computer in the event that the communications link has been idle for a period of time. The protected keepalive message is not a re-key request by the local computer to renegotiate the policy/key(s) of the secured communications link to the In-

ternet. In one embodiment, the protected keepalive message is a protected ISAKMP/Oakley command to which a protected acknowledgement must be supplied. If a protected acknowledgement is received from the remote box by the local box in response to the protected keepalive message, then it is assumed that the remote box is still reachable. However, if the protected acknowledgement is not received from the remote box in response to the protected keepalive message, then it is assumed that their remote box is no longer reachable. In this case, the secured communications link between the remote box and the local box is terminated by the local box.

BEST AVAILABLE COPY

EP 0 999 673 A2

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates generally to the field of data communications and, more specifically, the present invention relates to data communications through the Internet.

Background Information

[0002] The traditional workplace is generally thought of as a single location to which all employees commuted and worked during the day. With the explosion of technology, the definition of the workplace is expanding to include telecommuters as well as employees that work while traveling. In addition, employees may often need the ability to login remotely from their home or laptop computer systems to their employer's corporate networks for any number of reasons including accessing or transferring files or simply checking their electronic mail.

[0003] Figure 1 shows a computer system 101 remotely connected to a local area network (LAN) 131. As shown in Figure 1, computer system 101 is coupled to LAN 131 through a modem 103. Modem 103 is connected to modem 105 through a connection 127. Modem 105 is connected to a LAN bus 107, to which a plurality of other network resources are attached. For example, Figure 1 shows that computer systems 113 and 117 are coupled to LAN bus 107 through network interfaces 111 and 115, respectively.

[0004] A disadvantage with the setup described above for remotely coupling computer system 101 to corporate LAN 131 through the modems 103 and 105 is that connection 127 is typically a telephone connection through a public switched telephone network. Thus, if computer system 101 is located a great physical distance away from LAN 131, connection 127 may be a long distance telephone call, which could be quite expensive if used often or for long periods of time.

[0005] Figure 1 also shows that in the alternative, computer system 101 may be coupled to LAN 131 through the Internet 119. As shown in Figure 1, computer system 101 connects to an Internet service provider (ISP) 121 through connection 133. Typically, connection 133 is a local telephone call, which is more cost-effective in comparison with connection 127 in the event that connection 127 is a long distance telephone call. Figure 1 shows that ISP 121 is connected to a gateway system 109 through a connection 129 through the Internet 119. Gateway system 109 is connected to LAN 131 through LAN bus 107.

[0006] There are a variety of different protocols that may be used for connection 129 between ISP 121 and gateway system 109. One such example protocol is the Point-to-Point Tunnel Protocol (PPTP). A shortcoming

of this protocol is that it does not provide complete security in connection 129. As is known to those skilled in the art, the control channel of a PPTP connection is not encrypted. Consequently, it would be relatively easy for an intruder 125 to intercept the non-protected communications in connection 129 between ISP 121 and gateway system 109 and conceivably eavesdrop on communications, disrupt communications, or possibly even masquerade as one of the two parties.

[0007] One known protocol providing secured communications through the Internet 119 is the Internet Security Association and Key Management Protocol (ISAKMP)/Oakley protocol combined with Internet Protocol Security (IPSec). ISAKMP/Oakley is used for key management and IPSec is used for transferring encrypted data. As is known to those skilled in the art, the ISAKMP/Oakley protocol was designed to be used primarily for providing secured static host to host communications through the Internet 119 between networks that are not shut down often. For example, a pair of networks such as LAN 131 could communicate securely through the Internet 119 using the ISAKMP/Oakley protocol with IPSec. When designing the ISAKMP/Oakley protocol, it was assumed that the secured host to host (e.g. firewall to firewall) communications through the Internet 119 between networks would be relatively static. That is, the connections between the networks would remain active for relatively long periods of time and therefore would not be dropped frequently.

[0008] One disadvantage of using the ISAKMP/Oakley protocol with IPSec in the example illustrated in Figure 1 is that computer system 101 accesses the Internet 119 through modem 103. As is known to those skilled in the art, it is known that modem connections to the Internet 119 may drop often. For example, if connection 133 is on a noisy telephone line or if for example connection 133 includes the call waiting service, connection 133 could be dropped unexpectedly. As is known to those skilled in the art, the ISAKMP/Oakley protocol does not provide a keepalive feature. Consequently, LAN 131 would not be aware that computer system 101 was no longer reachable until the connection between computer system 101 and LAN 131 times out. Generally, ISAKMP/Oakley connections time out after attempts to renegotiate the policy and keys used to secure the communications link have failed. It is appreciated that the attempts to renegotiate the policy and keys to secure communications under the ISAKMP/Oakley protocol are computationally intensive operations and are therefore not performed at a high enough frequency to detect quickly and reliably that computer system 101 is no longer reachable through Internet 119.

SUMMARY OF THE INVENTION

[0009] A method of verifying the reachability of a remote box from a local box is disclosed. In one embodiment, the method includes the steps of establishing a

protected Internet communications link between the local box and the remote box. A protected keepalive message is transmitted to the remote box from the local box. The protected Internet communications link is terminated if the remote box fails to transmit to the local box a protected acknowledgement message in response to the protected keepalive message. Additional features and benefits of the present invention will become apparent from the detailed description, figures and claims set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The present invention is illustrated by way of example and not limitation in the accompanying figures.

[0011] Figure 1 is an illustration of a remote computer system accessing a LAN through a modem.

[0012] Figure 2 is an illustration of a remote computer system accessing a LAN through the Internet using a modem with secured communications in accordance with teachings of one embodiment of the present invention.

[0013] Figure 3 is an illustration showing an example of a computer system that may be used in accordance with teachings of one embodiment of the present invention.

[0014] Figure 4 is a flow diagram illustrating steps performed to verify the reachability of a remote computer from a local computer in accordance with the teachings of one embodiment of the present invention.

DETAILED DESCRIPTION

[0015] Methods and apparatuses for verifying the reachability of a remote computer from a local computer are disclosed. The subject of invention will be described with reference to numerous details set forth below, and the accompanying drawings will illustrate invention. The following description and drawings are illustrative of the invention and are not to be construed as limiting the invention. Numerous specific details are described to provide a thorough understanding of invention. However, in certain instances, well-known or conventional details are not described in order not to unnecessarily obscure the present invention.

[0016] Figure 2 shows a computer system 101 coupled to a LAN 131 through the Internet 119 in accordance with the teachings of one embodiment of the present invention. In particular, Figure 2 shows a computer system 101 coupled to the Internet 119 through ISP 121 through connection 133 from modem 103. In one embodiment, a protected Internet communications link is established between ISP 121 and gateway system 109. In the embodiment depicted in Figure 2, the protected Internet communications link between ISP 121 and gateway system 109 includes the first and second channels 201 and 203, respectively. LAN 131 accesses the Internet 119 through gateway system 109.

In one embodiment, gateway system 109 is coupled to LAN bus 107, to which other LAN 131 resources are connected including modem 105 and computer systems 113 and 117 through network interfaces 111 and 115, respectively.

[0017] It will be appreciated herein that the term "Internet" refers to a network of networks that use a variety of protocols, such as for example the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol, and other protocols including the HTTP for Hypertext Markup Language (HTML) documents. The physical connections of the Internet 119 and other protocols and communication procedures of the Internet 119 are well known to those skilled in the art. Access to Internet 119 is typically provided by Internet service providers (ISPs) such as ISP 121 and gateway systems, such as gateway system 109. Users on client systems, such as for example computer system 101, computer system 113 and computer system 117, obtain access to the Internet 119 through ISPs such as ISP 121 or gateway systems such as gateway system 109. Access to the Internet 119 allows users of client computer systems to exchange information, receive and send electronic mail, view electronic documents, etc..

[0018] It is noted that while the embodiment illustrated in Figure 2 depicts that computer system 101 is coupled to the Internet 119 through a "modem" 103, it is appreciated that the interface of computer system 101 to Internet 119 through modem 103 may be an analog modem, an Integrated Services Digital Network (ISDN) modem, cable modem, satellite transmission interface, Digital Subscriber Line (DSL) modem, or other interfaces for coupling a computer system or box to other computer systems or boxes.

[0019] Computer systems 113 and 117 are shown in the embodiment illustrated in Figure 2 to be coupled to LAN bus 107 through network interfaces 111 and 115, which may be an Ethernet network interfaces or other known network interfaces. In one embodiment, LAN bus 107 is coupled to gateway system 109, which may provide firewall and other Internet related services for LAN 131. In one embodiment, gateway system 109 may be a conventional server computer system, or another type of box including for example an Extranet switch that provides Internet 119 access for LAN 131.

[0020] Figure 3 shows one embodiment of a conventional computer system 301 that may be included in computer systems 101, 113 and 117 or gateway system 109 of Figure 2. It will also be appreciated that a computer system 301 may be used to perform many of the functions of Internet service provider, such as for example ISP 121 or the functions of remote and local boxes in accordance with the teachings of the present invention. The computer system 301 interfaces to external systems or boxes through the modem or network interface 319.

[0021] Although modems and network interfaces have been separately illustrated in Figure 2, such as for

example modems 103 and 105 and network interfaces 111 and 115, it will be appreciated that the modem or network interface 319 may be considered in some instances to be part of computer system 301. This modem or network interface 319 may be an analog modem, ISDN modem, cable modem, DSL modem, token ring interface, Ethernet interface, satellite transmission interface, or other interfaces for coupling a computer system or box to other computer systems or boxes. As also shown in Figure 3, a carrier wave signal 321 is received/transmitted by modem or network interface 321 for communications with computer system 301.

[0022] In the embodiment illustrated in Figure 3, computer system 301 includes a processor 303, which may be a conventional microprocessor such as for example an Intel x86 or Pentium family microprocessor, a Motorola 68K or PowerPC family microprocessor, or the like. Memory 305 is coupled to processor 303 by a bus 307. Memory 305 may be dynamic random access memory (DRAM) and may include static random access memory (SRAM). Bus 307 couples processor 303 to memory 305 and also to mass memory 313 and to display controller 309 and the I/O (input/output) controller 315.

[0023] Mass memory 313 is often a magnetic hard disk, an optical disk, or another form of storage for large amounts of data. Some of this data may be written by a direct memory access process into memory 305 during execution of software and computer system 301. It is appreciated that software may also be transmitted or received via modem or network interface 319. For purposes of this specification, the term "computer readable medium" shall be taken to include any medium that is capable of storing or encoding a sequence of instructions for execution by a processor and causes the processor to perform the methodologies of the present invention. The term "computer readable medium" shall be taken to include, but not be limited to solid-state memories, optical and magnetic disks, carrier wave signals, or the like.

[0024] It will be appreciated that computer system 301 is merely one example of many possible computer systems that have different architectures. For example, WINTEL systems, systems that include Intel microprocessors running the Microsoft Windows operating system, often have multiple buses, one of which may be considered a peripheral bus. Networked computers may also be considered to be a computer system that may be used with the present invention. Network computers may not include a hard disk or other mass memory 313, and the executable programs are loaded from a network connection into memory 305 for execution by processor 303. A typical computer system will usually include at least processor 303, memory 305 and a bus 307 for coupling memory 305 to processor 303.

[0025] It will also be appreciated that computer system 301 is controlled by operating system software that includes a file management system, such as a disk op-

erating system, which is part of the operating system software. One example of an operating system software with its associated file management system software is the operating system known as Windows from Microsoft Corporation of Redmond Washington, and its associated file management system, including Windows Explorer. The file management system is typically stored in the mass memory 313 and causes processor 303 to execute the various steps required by the operating system to input and output data and to access data in memory, including accessing files in mass memory 313.

[0026] Referring back to the embodiment depicted in Figure 2, a user on computer system 101 is able to access LAN 131 securely and remotely through a protected communications link through Internet 119. Conversely, users on LAN 131 are able to access computer system 101 securely and remotely through the protected Internet communications link. In one embodiment, the protected communications link through Internet 119 between computer system 101 and gateway system 109 employs the Internet Security Association and Key Management Protocol (ISAKMP)/Oakley protocol to secure communications. As is known to those skilled in the art, ISAKMP/Oakley is the key management protocol designed by the Internet Engineering Task Force (IETF) Internet Protocol Security (IPSec) working group.

[0027] As is known to those skilled in the art, ISAKMP/Oakley provides a framework for authentication, security association negotiation and key management for the protected Internet communications link between computer system 101 and gateway system 109. Specifically, ISAKMP provides a framework for authentication and key exchange, but does not define them. Oakley describes a series of key exchanges and details the services provided by each. In one embodiment, the Oakley protocol defines a generic key exchange protocol employing the well-known and complex Diffie-Hellman key exchange algorithm. As such, the periodic renegotiation of the keys used to secure the protected Internet communications link between computer system 101 and gateway system 109 is a computationally intense operation.

[0028] Information describing the ISAKMP/Oakley protocol may be found in the following Internet Draft working documents: Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP)," <ftp://ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-10.txt>; Orman, "The OAKLEY Key Determination Protocol," <ftp://ietf.org/internet-drafts/draft-ietf-ipsec-oakley-02.txt>; and Harkins & Carrel, "The Internet Key Exchange (IKE)," <ftp://ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-oakley-08.txt>. These documents are incorporated herein by reference.

[0029] In the embodiment depicted in Figure 2, the protected communications link through the Internet 119 includes a first channel 201 and a second channel 203 between ISP 121 and gateway system 109. As a result, two protected links 213 and 215 are formed between

computer systems 101 and gateway system 109. In the embodiment illustrated in Figure 2, protected link 213 is formed between computer system 101 through modem 103, through connection 133 to ISP 121, through channel 203 to gateway system 109. Similarly, protected link 215 is formed between computer system 101 through modem 103, through connection 133 to ISP 121, through channel 203 to gateway system 109.

[0030] In one embodiment, protected link 215 and channel 201 carry control traffic used for, among other things, negotiating and renegotiating the policy/key(s) 211 used for securing channels 201 and 203 of the protected Internet communications link. In one embodiment, the ISAKMP/Oakley traffic including policy/key(s) 211 is carried in channel 201. In one embodiment, all traffic in channel 201 is encrypted and therefore protected. In one embodiment, channel 203 is also a protected channel and protected link 213 with channel 203 carry protected data 205 using IPsec between ISP 121 gateway system 109. In one embodiment, channel 203 carries IPsec tunnel traffic.

[0031] In accordance with one embodiment of the present invention, when the protected Internet communications link is established between computer system 101 and gateway system 109 of LAN 131, the policy/key(s) 211 used for protecting channels 201 and 203 are negotiated under the ISAKMP/Oakley protocol. In one embodiment, the established secure and authenticated channel through which computer system 101 and gateway system 109 communicate through Internet 119 is called a security association under the ISAKMP/Oakley protocol. After the secured Internet communications link has been established, computer system 101 and LAN 131 are able to communicate securely. Since channels 201 and 203 are secured, it is extremely difficult for an intruder 125 to eavesdrop, interfere with or disrupt communications between computer system 101 and LAN 131.

[0032] In one embodiment, the policy/key(s) 211 used under the ISAKMP/Oakley protocol are renegotiated periodically to maintain the security of the protected Internet communications link between computer system 101 and gateway system 109. In one embodiment, the policy/key(s) 211 are renegotiated after a predetermined amount of time has elapsed since the previous time the policy/key(s) 211 have been negotiated. In another embodiment, the policy/key(s) 211 are renegotiated after a predetermined amount of data has been transferred through the protected Internet communications link since the last time the policy/key(s) 211 have been negotiated.

[0033] As mentioned earlier, since the process to establish the policy/key(s) 211 is a computationally intense procedure, there is a practical limit on how often the renegotiation process can be performed. As is appreciated to those skilled in the art, the frequency in which the renegotiation process under ISAKMP/Oakley typically occurs is on the order of only every several times per

day. Otherwise, computer system 101 and/or gateway system 109 would be unduly burdened with having to recompute the policy/key(s) 211 under the Diffie-Hellman key exchange algorithm.

5 In the event that a remote computer or box fails to respond to a re-key request under the ISAKMP/Oakley protocol, it is assumed that the remote computer box is no longer reachable and the protected Internet communications link and associated security association under the ISAKMP/Oakley protocol is torn down.

[0034] As described above, computer system 101 accesses Internet 119 through a modem connection from modem 103. Consequently, there is a reasonable possibility that the connection 133 between modem 103 and ISP 121 may drop at a frequency higher than that which could be quickly and practically detected by gateway system 109 by simply relying on a timeout exception occurring after a ISAKMP/Oakley re-key or renegotiation request. Indeed, as described above, the renegotiation process is typically performed only several times per day. Unfortunately, the ISAKMP/Oakley protocol was originally designed primarily to secure Internet communications between systems that do not go down regularly. The ISAKMP/Oakley protocol was not originally designed for users logging into networks using unreliable modem connections. Thus, if a connection 133 is unexpectedly dropped for any reason and the user of computer system 101 attempts to re-access LAN 131 through a secured ISAKMP/Oakley connection through Internet 119, there is a possibility that the user may be unable to re-login to LAN 131 because gateway system 109 is unaware that the previous connection 133 between modem 103 and ISP 121 has been dropped.

[0035] In particular, under ISAKMP/Oakley, gateway system 109 will not have torn down the security association of the previous protected Internet communications link. Consequently, if the user of computer 101 is entitled to only one secured link to LAN 131 and under ISAKMP/Oakley, the user will be unable to login until the previous secured association is torn down. However, under ISAKMP/Oakley, the security association will not be torn down until the above described timeout exception occurs after the renegotiation request, which in some instances may occur only several times a day.

[0036] In another situation, it is appreciated that a router or other hardware device contained in Internet 119 through which communications between computer system 101 and LAN 131 are carried may also fail. In this example, connection 133 between modem 103 and ISP 121 may not have been unexpectedly dropped, but nevertheless, computer system 101 is not reachable from LAN 131 and vice versa. It is appreciated that in this situation, gateway system 109 may also be unaware that computer system 101 is not reachable for many hours until the above described timeout exception occurs after the renegotiation request.

[0037] In order to address the above described problem, one embodiment of the present invention transmits

a protected keepalive message 209 to the remote computer system or box from the local computer system or box. In one embodiment, the local box may be computer system 101 and the remote box may be gateway system 109. In another embodiment, the local box may be gateway system 109 and the remote box may be computer system 101. Indeed, the present invention is applicable to any combination of local and remote boxes between which there are secured communications through the Internet 119.

[0038] In one embodiment, the protected keepalive message is a message to which it is mandatory to send a protected acknowledgement signal. In an embodiment implying the ISAKMP/Oakley protocol, the keepalive message 209 is a protected ISAKMP/Oakley message sent from the local box to the remote box. In one embodiment, the protected ISAKMP/Oakley message is a message to which the remote box must reply with a protected acknowledgement message 207. In one embodiment, the protected keepalive message 209 and the protected acknowledgement message 207 are transmitted through protected link 215 and the first channel 201 between ISP 121 and gateway 109. Since the protected keepalive message 209 and the protected acknowledgement message 207 are secured under the ISAKMP/Oakley protocol, it is appreciated that it is extremely difficult for an intruder 125 to intercept or manipulate protected keepalive message 209 and protected acknowledgement 207 in accordance with teachings of the present invention.

[0039] In one embodiment, since the ISAKMP/Oakley protocol was not implemented with a keepalive message, another ISAKMP/Oakley non-keepalive command is used as a keepalive message 209. In one embodiment, an ISAKMP/Oakley quick mode message including an invalid proposal and transform is used as a keepalive message 209 in accordance with the teachings of the present invention. In one embodiment, this quick mode message is transmitted by the local box to the remote box after the communications link has been idle for a period of time. In one embodiment, this keepalive message 209 is transmitted by the local box after, for example, one minute has passed when no traffic has been sent to or received from the remote box. Under the ISAKMP/Oakley protocol, the remote box must reply back to the local box by sending a protected acknowledgement 207 back to the local box.

[0040] In the event that the local box does not receive the protected acknowledgement message 207 back from the remote box after having transmitted the protected keepalive message 209, is assumed that the remote box is no longer reachable. As discussed above, this may occur if the modem connection between modem 103 and ISP 121 is dropped or if for example a router or other piece of hardware in Internet 119 providing the protected Internet communications link fails. As a result, the local box can terminate the protected Internet communications link between computer system 101

and gateway system 109 in accordance with the teachings of the present invention. In one embodiment, the local box tears down the associated security association under the ISAKMP/Oakley protocol.

[0041] Figure 4 is a flow diagram illustrating steps performed in accordance with the teachings of one embodiment of the present invention. It is appreciated that the steps performed in accordance with the teachings of the present invention may be implemented as software, firmware, hardware, etc., in the local and remote boxes. Processing step 403 shows that secured communications are established between a local box and a remote box through first and second channels through the Internet. Processing step 405, shows that the policy/key(s) between the local box and the remote box are negotiated or renegotiated to protect the secured first and second channels.

[0042] Processing decision step 407 shows that it is next determined whether there have been any communications between the local box and the remote box in the past N minutes. Stated differently, it is determined whether the secured communications between the local box and the remote box have been idle in the past N minutes. Is appreciated that N may be chosen to be a value that would on the one hand enable a dropped connection between the remote box and local box to be detected in a relatively short period of time, but on the other hand would not unduly burden the secured communications link between the local and remote boxes with keep-alive traffic.

[0043] If there has been communications traffic between the local box and remote box in the past N minutes, then processing decision step 409 shows that it is next determined whether X Kbytes have been transferred between the remote box and local box or if Y hours have lapsed since the most recent time that the policy/key(s) have been negotiated. It is appreciated that X or Y are chosen to be values that enable the ISAKMP/Oakley policy/key(s) to be changed at adequate intervals for security reasons while at the same time X or Y are chosen to be values that t would not excessively burden the remote and/or local boxes with the computationally intensive processing required to renegotiate the policy/key(s).

[0044] If the conditions of processing decision step 409 are met, then processing loops back to processing step 405 where the policy/key(s) are renegotiated to protect the secured communications link. If the conditions of processing decision step 409 are not met, then processing loops back to processing decision step 407 where it is again determined whether there have been any communications between the remote and local boxes within the past N minutes.

[0045] In the event that there have not been any communications between the local and remote boxes in the past N minutes, then processing from processing decision step 407 proceeds to processing step 411. Processing step 411 shows that a protected keepalive

message is sent from the local box to the remote box through the first channel. As discussed above, the keep-alive message is a message to which a protected acknowledgement must be sent. Accordingly, processing decision step 413 shows that it is next determined whether a protected acknowledgement to the keepalive message has been received from the remote box. If so, then processing loops back to processing decision step 407. In this case, it is assumed that the remote box is reachable. However, if the protected acknowledgement is not received, then processing proceeds to processing step 415 where it is shown that the secured communications between the local and remote boxes are discontinued. Indeed, if the protected acknowledgement is not received in processing decision step 413, it is assumed that the remote box is no longer reachable from the local box.

[0046] The foregoing discussion has provided numerous examples of the present invention. It will be appreciated that various modifications and changes may be made thereto without departing from a broader spirit and scope of the present invention as set forth in the appended claims.

Claims

1. A method of verifying reachability of a remote box from a local box, the method comprising:

establishing a protected Internet communications link between the local box and the remote box;
transmitting a protected keepalive message to the remote box from the local box; and
terminating the protected Internet communications link if the remote box fails to transmit to the local box a protected acknowledgement message in response to the protected keep-alive message.

2. A method of maintaining a protected Internet communications link between a local box and a remote box, the method comprising:

renegotiating periodically a policy and a key between the local box and the remote box to secure the protected Internet communications link;
transmitting a protected keepalive message to the remote box from the local box; and
terminating the protected Internet communications link if the remote box fails to transmit to the local box a protected acknowledgement message in response to the protected keep-alive message.

3. A computer readable medium having sequences of

instructions stored therein, which when executed cause a processor to perform a method comprising:

establishing a protected Internet communications link between a local box and a remote box;
transmitting a protected keepalive message from the local box to the remote box; and
terminating the protected Internet communications link if the remote box fails to transmit to the local box a protected acknowledgement message in response to the protected keep-alive message.

4. The method of claim 1 or 2 or the medium of claim 3, wherein transmitting the protected keepalive message to the remote box from the local box is performed after the protected Internet communications link has been idle.

5. The method of claim 1 or 2 or the medium of claim 3, wherein establishing the protected Internet communications link between the local box and the remote box includes:

establishing a protected first channel through the Internet between the local box and the remote box through which control information is transferred; and
establishing a protected second channel through the Internet between the local box and the remote box through which data information is transferred.

6. The method or medium of claim 5 wherein the protected keepalive message and the protected acknowledgement message are transmitted through the protected first channel between the local and remote boxes.

7. The method of claim 1 or 2 or the medium of claim 3, wherein it is mandatory that the remote box transmit the protected acknowledgement message to the local box in response to receiving the protected keepalive message and wherein establishing the method of claim 1 wherein establishing the protected Internet communications link between the local box and the remote box, includes negotiating a policy and a key between the local box and the remote box to secure the protected Internet communications link.

8. The method of claim 1 or the medium of claim 3, wherein it is mandatory that the remote box transmit the protected acknowledgement message to the local box in response to receiving the protected keep-alive message and wherein establishing the protected Internet communications link between the local box and the remote box, includes negotiating a

policy and a key between the local box and the remote box to secure the protected Internet communications link.

9. The method or medium of claim 8 further comprising renegotiating the policy and the key between the local box and the remote box periodically to secure the protected Internet communications link. 5
10. The method or medium of claim 9 wherein renegotiating the policy and the key between the local box and the remote box periodically to secure the protected Internet communications link, is performed after a predetermined period of time has elapsed. 10
15
11. The method or medium of claim 9 wherein renegotiating the policy and the key between the local box and the remote box periodically to secure the protected Internet communications link, is performed after a predetermined amount of information has been transferred between the local box and the remote box. 20
12. The method of claim 1 or 2 or the medium of claim 3, wherein establishing the protected Internet communications link between the local box and the remote box, is performed using the Internet Security Association and Key Management Protocol (ISAKMP)/Oakley protocol. 25
30
13. The method or medium of claim 12 wherein the protected keepalive message is a protected ISAKMP/Oakley message to which the protected acknowledgement message must be transmitted from the remote box in response. 35
14. The method or medium of claim 13 wherein the protected ISAKMP/Oakley message is a protected ISAKMP/Oakley quick mode message with an invalid proposal and transform. 40
15. The method of claim 1 or 2 or the medium of claim 3, wherein the protected Internet communications link between the local box and the remote box includes an ISAKMP/Oakley security association. 45
16. The method or medium of claim 15 wherein terminating the protected Internet communications link, includes tearing down the ISAKMP/Oakley security association. 50
17. The method or medium of claim 9 wherein transmitting the protected keepalive message to the remote box from the local box, is performed separately from renegotiating the policy and the key between the local box and the remote box periodically to secure the protected Internet communications link. 55

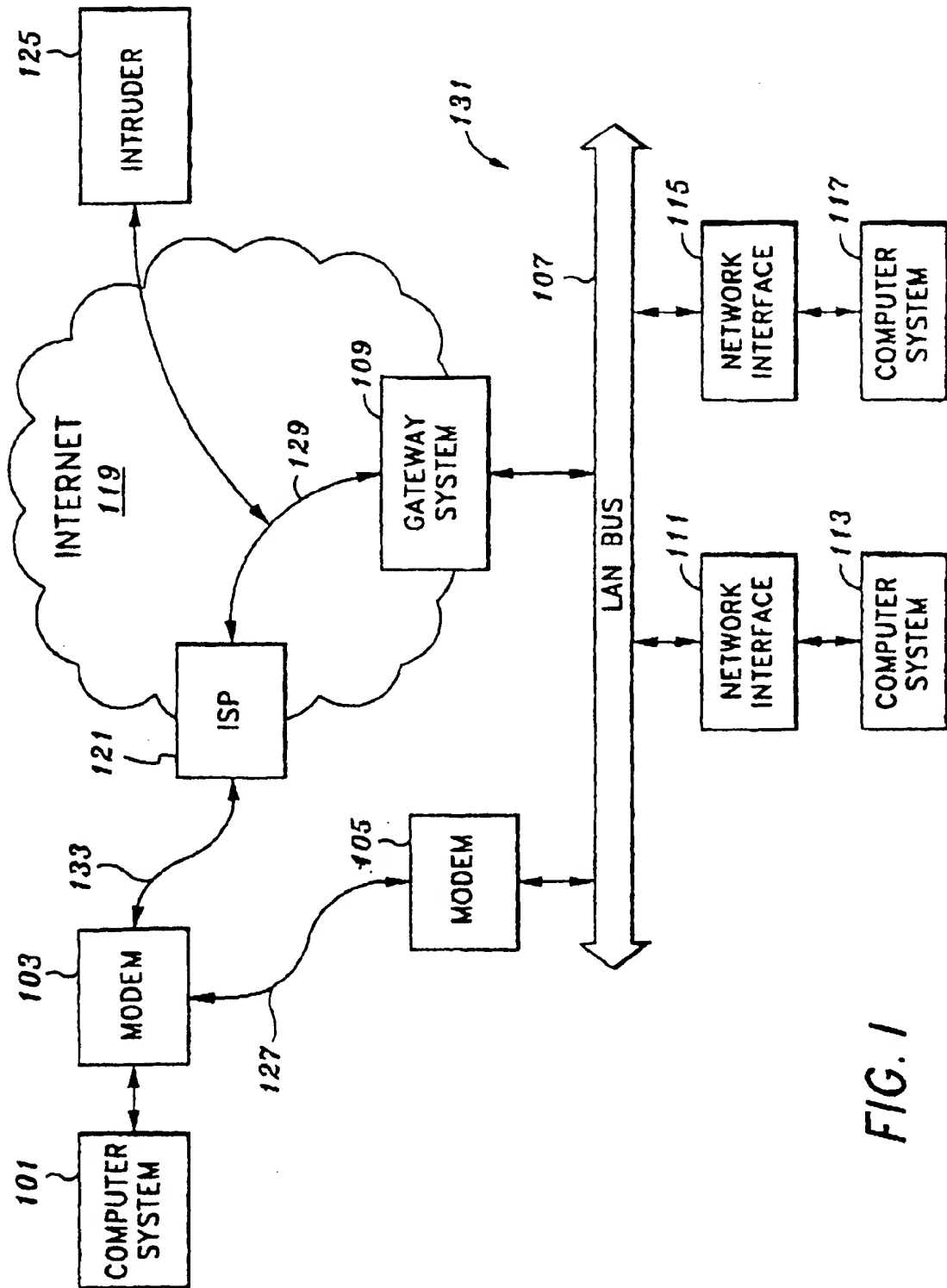


FIG. 1

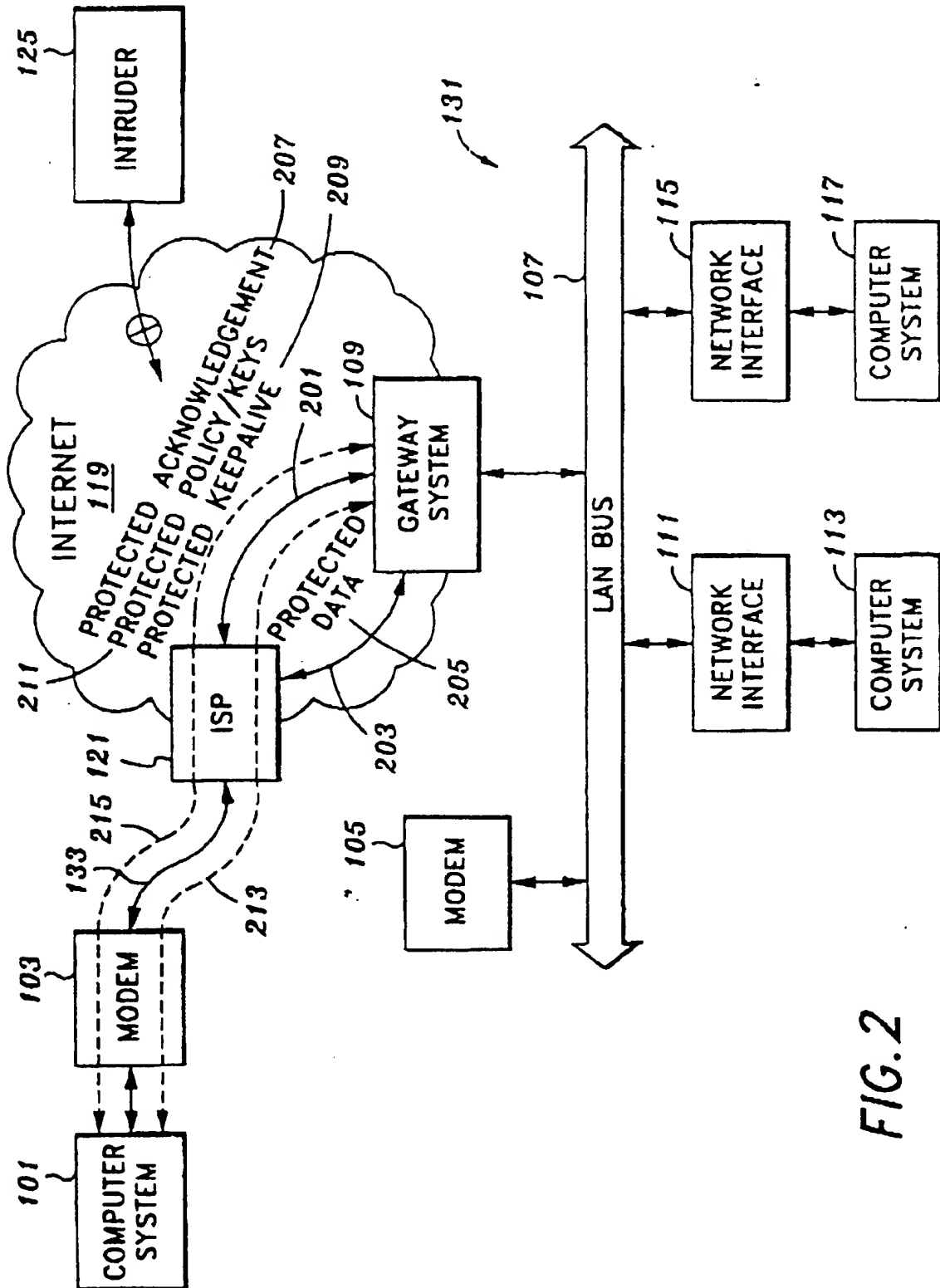


FIG. 2

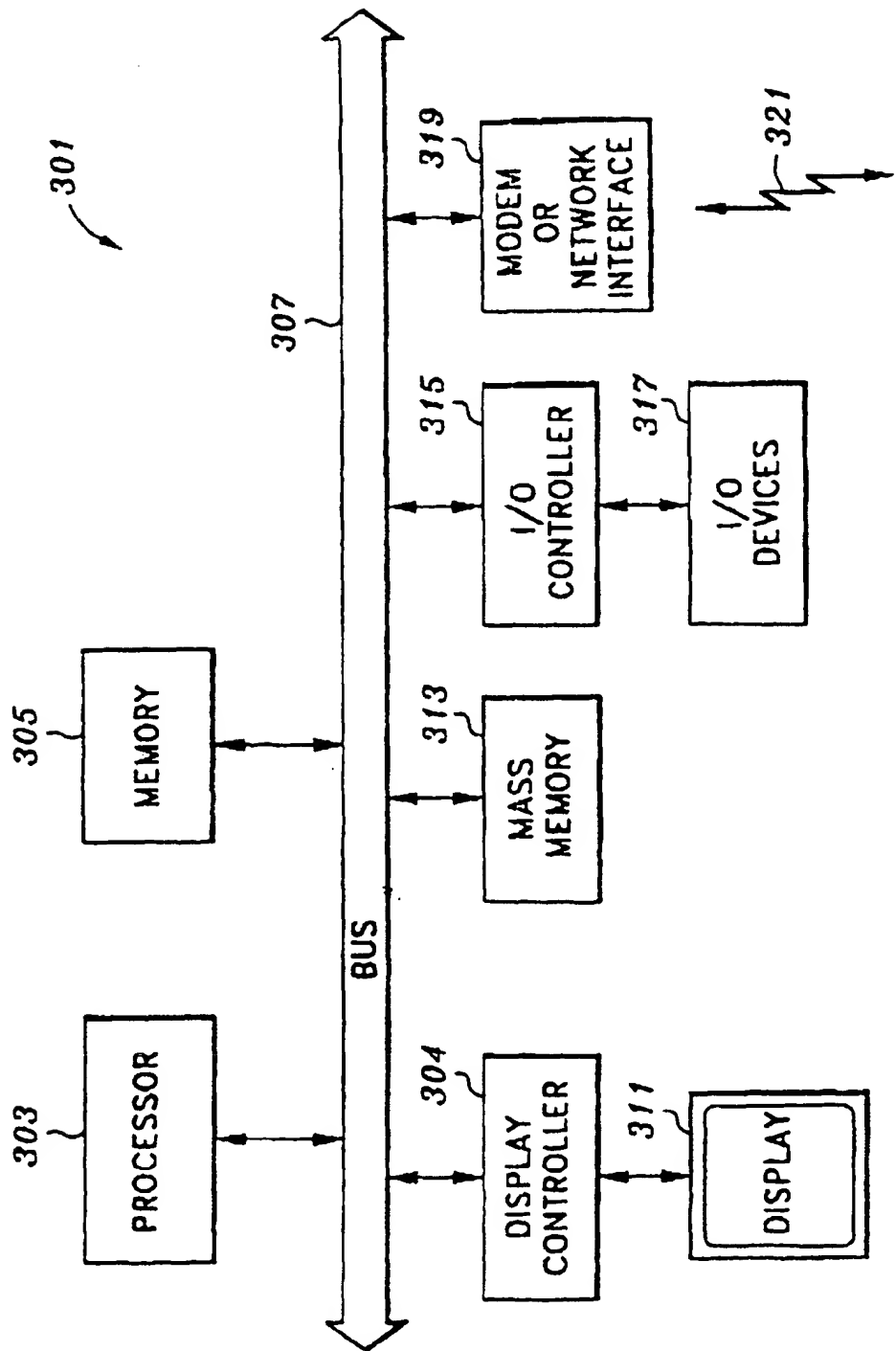


FIG. 3

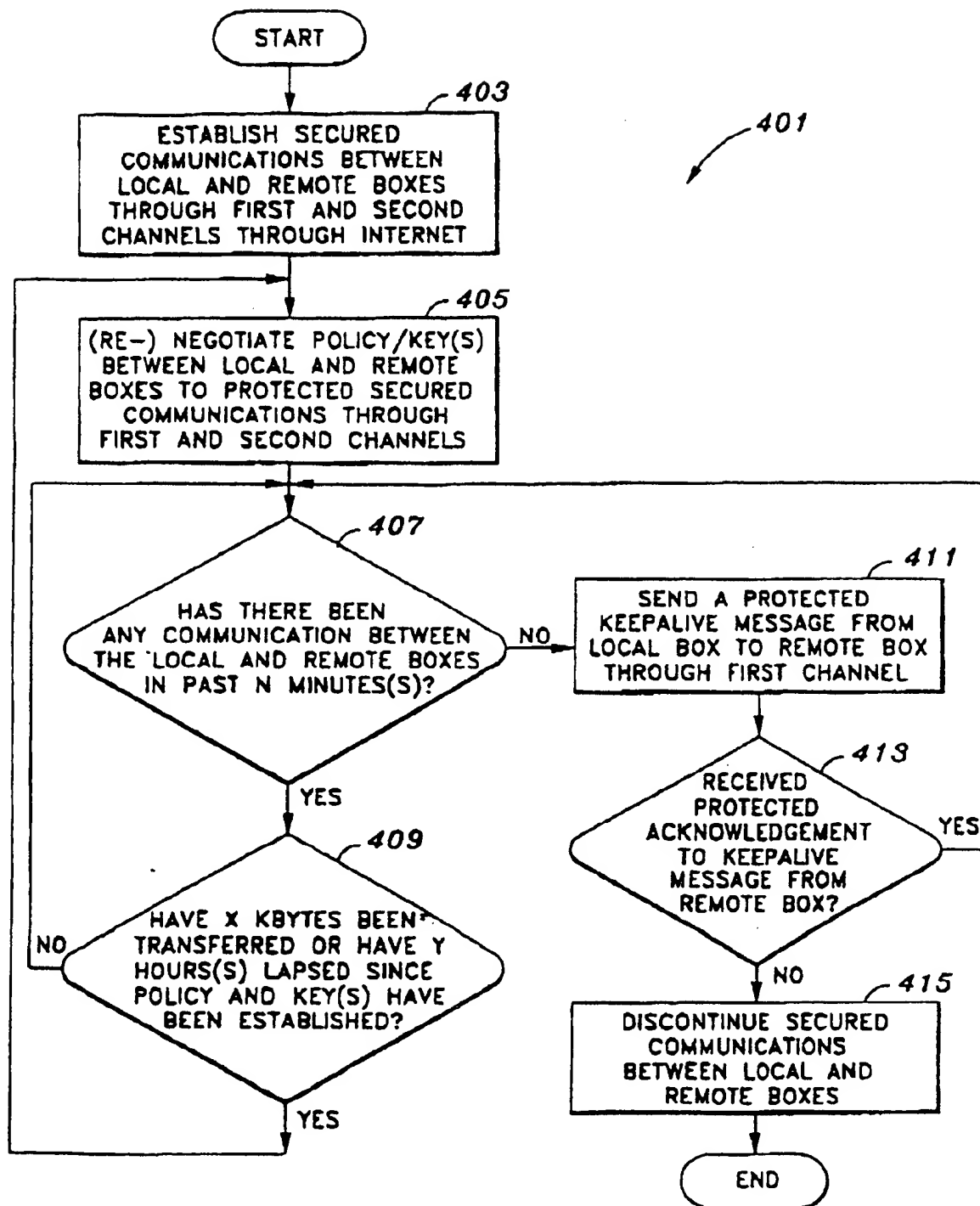
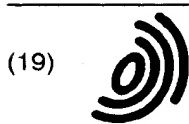


FIG. 4



(19)

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 999 673 A3

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
12.12.2001 Bulletin 2001/50

(51) Int Cl.7: **H04L 12/58, H04L 29/06,
H04L 12/26**

(43) Date of publication A2:
10.05.2000 Bulletin 2000/19

(21) Application number: **99308689.1**

(22) Date of filing: **02.11.1999**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE**
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **03.11.1998 US 185056**

(71) Applicant: **Nortel Networks Limited
Montreal, Quebec H2Y 3Y4 (CA)**

(72) Inventors:
• **Mamros, Shawn
Arlington, Massachusetts 02476 (US)**
• **Hannigan Kerry M
Boston, Massachusetts 02215 (US)**

(74) Representative: **Maury, Richard Philip et al
Sommerville & Rushton,
Business Link Building,
45 Grosvenor Road
St. Albans, Herts AL1 3AW (GB)**

(54) **Protected keep alive message through the internet**

(57) A method and apparatus for determining the reachability of a remote computer from a local computer through a secured communications link through the Internet. In one embodiment, the secured ISAKMP/Oakley communications link is established between a remote computer and a local computer through the Internet. A protected keepalive message is transmitted by the local computer to the remote computer in the event that the communications link has been idle for a period of time. The protected keepalive message is not a re-key request by the local computer to renegotiate the policy/key(s) of the secured communications link to the In-

ternet. In one embodiment, the protected keepalive message is a protected ISAKMP/Oakley command to which a protected acknowledgement must be supplied. If a protected acknowledgement is received from the remote box by the local box in response to the protected keepalive message, then it is assumed that the remote box is still reachable. However, if the protected acknowledgement is not received from the remote box in response to the protected keepalive message, then it is assumed that their remote box is no longer reachable. In this case, the secured communications link between the remote box and the local box is terminated by the local box.

EP 0 999 673 A3



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 8689

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y A	US 5 553 239 A (HEATH DAVID M ET AL) 3 September 1996 (1996-09-03) * abstract * * figure 6 * * column 3, line 38 - line 56 * * column 7, line 52 - column 8, line 8 * * claims 1,8 *	1-3 4-17	H04L12/58 H04L29/06 H04L12/26
Y A	US 5 633 933 A (AZIZ ASHAR) 27 May 1997 (1997-05-27) * abstract * * figures 2-4 * * claims 1-3 *	1-3 4-17	
Y	WO 97 26735 A (RAPTOR SYSTEMS INC) 24 July 1997 (1997-07-24) * abstract * * page 2, line 22 - page 3, line 25 *	1-3	
A	US 5 822 434 A (CARONNI GERMANO ET AL) 13 October 1998 (1998-10-13) * abstract * * figure 2 * * claims 1-11 *	1-17	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L
The present search report has been drawn up for all claims			
Place of search MUNICH		Date of completion of the search 17 October 2001	Examiner Wolf, W
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 33 82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 99 30 8689

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

17-10-2001

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5553239	A	03-09-1996	NONE	
US 5633933	A	27-05-1997	US 5588060 A	24-12-1996
			EP 0693836 A1	24-01-1996
			JP 8008895 A	12-01-1996
			US 5668877 A	16-09-1997
			US 6091820 A	18-07-2000
			US 6026167 A	15-02-2000
WO 9726735	A	24-07-1997	AU 1748797 A	11-08-1997
			WO 9726735 A1	24-07-1997
			US 5825891 A	20-10-1998
US 5822434	A	13-10-1998	NONE	

EPO FORM P0439

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☒ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.